~~S-E-C-R-E-T~~

IBSEC-CSS-M-7
4 February 1969

COMPUTER SECURITY SUBCOMMITTEE

OF THE

UNITED STATES INTELLIGENCE BOARD

SECURITY COMMITTEE

Minutes of Meeting
Held at CIA Headquarters
Langley, Virginia
4 February 1969

1. The seventh meeting of the Computer Security Subcommittee of the USIB Security Committee was held on 4 February 1969 between 1330 and 1520 hours in Rm. 4E-64 CIA Headquarters Building. In attendance were:

[redacted] STAT
Mr. Richard F. Kitterman, State, Member
[redacted] STAT
Mr. Thomas A. Eccleston, Army, Member
Mr. Robert C. Allen, Navy, Member
Lt. Col. Charles V. Burns, Air Force, Member
[redacted] STAT
Mr. Raymond J. Brady, AEC, Member
[redacted] STAT
Lt. Col. William D. Marsland, Jr., JCS/JCCRG, Observer
[redacted] STAT
Mr. Cleddie B. Lanier, State
[redacted] STAT
Maj. James B. Walton, Army
Mr. Louis J. Martin, Army
Mr. Carl R. Lambert, Navy

~~S-E-C-R-E-T~~

Group 1
Excluded from automatic
downgrading and
declassification

2. The security level of the meeting was announced as Top Secret non-codeword.

3. Approval of Minutes: The minutes of the 18 December 1968 meeting were approved as written.

4. Briefing on CIA Time-Sharing System Security: Mr. [redacted] Security Officer of a principal CIA computer component, provided the Subcommittee with a briefing of the security features of one of the CIA time-sharing systems. [redacted] spoke of the physical, personnel, and procedural aspects of the security of this system which includes several remote terminal sites in the CIA Headquarters Building. He outlined basic protect features of the system including log-on procedures, component operator control of the system, directory and file (read only or read/write) key words. The briefing served to provide members with a picture of protect features developed in the CIA system, and will be followed in subsequent meetings by descriptions of security features in other community time-sharing systems.

STAT

STAT

5. Problem Area Consolidation Report: The Chairman advised the Subcommittee that he had, as mentioned during the previous meeting, edited the consolidated outline of computer security problem areas and forwarded it to the Chairman of the Security Committee as a report with a cover memorandum indicating that individual problems would be explicitly defined as addressed by the Subcommittee. Further, he indicated that he had reported to the Security Committee at its meeting on 4 February on the undertaking. Copies of the Problem Area Consolidation Report were distributed to Subcommittee members at the instant meeting.

6. Problem Priority Assignment: The Chairman stated that the next step in addressing the computer security problem areas was the determination of individual priorities among the problems listed. The Army has submitted its priority listing; other members were requested to provide their submissions by 20 February, so that this matter may be placed on the agenda for discussion at the next Subcommittee meeting.

7. Disc Degaussing: As indicated during the previous discussion of the feasibility of establishing a computer disc refurbishing facility, the Chairman prepared an outline for the information of members on the problem involved in downgrading or declassification of computer storage media, especially disc packs. A copy of the Chairman's working paper on this subject is attached to the minutes for member information.

8. The Chairman emphasized the importance of this problem within CIA by pointing out that currently that Agency is holding over 50 computer disc packs which are surplus to current requirements or are damaged and for security reasons cannot be returned to the manufacturer. The AEC representative pointed out that during the past month, his organization has had a similar problem involving the damaging of several computer disc packs containing classified material. Contact with IBM representatives at San Jose, California, reflected that the problem of replacing the platters on computer disc packs may be relatively simple and (as [redacted] of NSA indicated at the earlier meeting) may be significantly less costly than the purchase of a new disc pack. The DIA representative expressed his view that within his organization the disc pack declassification problem did not appear to be of major proportions. Mr. Lambert recalled an experience in 1964 at the Strategic Air Command where this downgrading of discs proved to be a costly exercise. The Navy representative indicated that his organization assumes certain risks in this regard, but welcomed a Subcommittee report in this area. STAT

9. One of the problems involved in studying the sanitization of storage media is the quantification of the risk involved when such media are downgraded after overwrite or other protection. The Chairman requested the NSA member's assistance in arranging a briefing of the Subcommittee by a person knowledgeable of any data retrieval tests conducted by that agency on storage media.

10. Although at the present time requests to downgrade storage media including disc packs are handled on an individual basis, the Subcommittee agreed that a standardized approach to the problem on the part of the community would help eliminate a

significant amount of the red tape involved in the current procedure. It is anticipated that the NSA representative will attempt to arrange such a briefing and that the Subcommittee will pursue this downgrading problem including consideration of refurbishment capabilities.

11. Other Business:

A. Membership List: The Chairman again reminded members that a firm list of participants in Subcommittee activities was needed to permit initiation of compartmented clearance requests. Each participating agency was requested to furnish the office of the Chairman by 20 February with the names of a member, an alternate, and a technical representative, their rank, organizational component, mailing address, and telephone number.

B. Inspection of Contractor Computer Facilities: Discussion of this item was deferred to the next meeting to permit members an opportunity to gather information on how various agencies are approaching the problem of computer security at contractor installations. The DoD representatives pointed out that the Defense Supply Agency has responsibility for industrial contractor security and suggested that DSA might provide a presentation at a future meeting on its approach to computer security inspections.

C. Computer Security Training Course: The NSA and DIA representatives provided additional information on the training course in computer security being planned at the Department of Defense Computer Institute under DSA sponsorship. It is anticipated that the pilot course will take place in about June 1969 and will be formatted in a manner similar to the interim schedule provided the Chairman at the 18 December meeting.

D. The Chairman announced that at the next Subcommittee meeting, Col. Marsland had offered to present a progress report on the security aspects of the JCCRG ad hoc Task Force addressing the problems involved in the co-location of the Intelligence Data Handling Systems and the Command and Control Centers. Col. Marsland will also attempt to arrange a briefing of the Subcommittee by appropriate JCS personnel on the security considerations

involved in the decision to introduce SIOP material into the AUTODIN network.

E. COINS Security Officer: [redacted] STAT of NSA was introduced to the Subcommittee as the newly appointed COINS Security Officer; he will be attending Subcommittee meetings in the future in an observer status.

12. The next meeting of the Computer Security Subcommittee is scheduled for 1330 hours on 4 March 1969 in Room 4E-64, CIA Headquarters.

[redacted] STAT

Chairman
Computer Security Subcommittee

Attachment

WORKING PAPER

The Sanitization of Computer Storage Media

1. Among the problem areas identified by the USIB Computer Security Subcommittee is the protection of computer storage media, e.g. disc file units, disc packs, drums, data cells, magnetic tapes, and even main memory. An important aspect of the protection of these media is the development of a method of sanitizing them, so that it is not necessary for the media themselves to retain permanently the highest security classification or most restrictive dissemination control of data stored thereon.

2. Acceptable means have been developed for degaussing magnetic computer tapes to permit their downgrading or declassification (except in one area). Specifications for degaussing equipment have been set forth and approved by appropriate authorities; the use of such equipment permits the declassification of such tapes.

3. During the past three years, large scale introduction of disc storage media, at least at CIA, have suggested a great need for developing an acceptable method for downgrading and/or declassifying disc packs, when such units have been used for storing classified data.

4. This need is particularly evident in two situations:

(a) When a leased or purchased disc pack becomes damaged, the manufacturer may repair or replace it, but in either case needs to assume control of the damaged disc, and therefore the contents thereon;

(b) with the introduction of new disc drive units, CIA has found itself in possession of surplus disc packs not usable on the new drives. Security considerations have not permitted the return of such surplus leased disc packs to the manufacturer, nor the disposal (other than by destruction) of surplus purchased packs.

It is also important to recognize that most disc packs, damaged or surplus, may have reserve tracks which cannot be overwritten.

5. The following alternatives are outlined as possible solutions to the problem:

(a) disposal: surplus and/or damaged packs may be destroyed, e.g. by melting;

(b) the disc packs may be retained in a surplus storage capacity "forever";

(c) overwrite procedures may be exercised, followed by a verification of the overwrite, and the disc pack may then be downgraded with an indeterminate degree of risk;

(d) heat treatment may be applied to the disc in conjunction with the overwrite; a similar but more practical approach may be the storing of the disc subsequent to overwrite procedures at the ambient temperature prevailing during normal system operations;

(e) the disc may be refurbished; i. e. the platters removed from the disc pack base and replaced; the used platters then destroyed in an appropriately secured manner. Such refurbishing may be accomplished either through a manufacturer, a contractor, inhouse, or by a centrally located community or government facility;

(f) at least conceptually, a capability may be developed of degaussing computer discs in a manner similar to that used and approved for magnetic tapes.

6. At the present time, disc packs are expensive; the IBM 2314 sells at $600 and rents at $20 per month. Destruction of surplus or damaged discs does not appear to be a satisfactory alternative, nor does the indefinite retention of such disc packs, since eventually disposal must be accomplished. This latter alternative also appears impractical from a cost viewpoint when the discs are leased.

7. While some evidence is available upon which evaluation of overwrite, heat and temperature treatments can be evaluated, the inherent risks in such alternatives are difficult to quantify.

8. While the risks involved in degaussing computer discs are difficult to project, it may be possible to compare them to those involved in the degaussing of tapes. The development of such a degaussing capability may be costly.

9. The risks involved in disc refurbishment from a security standpoint are nil, since the removal of used platters would be accomplished in a secure environment, and only the replacement of these disc packs would be done otherwise. The feasibility of refurbishment then appears to be a trade off between the cost involved in the refurbishment and the loss involved in disc destruction.